Mobile Hotspot Router (R526A) User Guide

Franklin Wireless R526A User Guide

www.franklinwireless.com / Version 03.28.2012

Table of Contents

Thank you for purchasing the Franklin Wireless R526A portable router. This device doesn't need wires, cables, or software to configure it through your Web browser.

This guide describes the browser Interface that allows you to configure the R526A. For information about setting up your device, device maintenance and care, etc., consult the printed Quick Start Guide that came with your device.

We recommend you read this manual before using the R526A.

Part 1

Using the R526A

Franklin Wireless

Charging the R526A Device

Note.

The battery should be fully charged before using the R526A for the first time. We recommend an initial charge time of approximately 2 hours. When fully charged, a solid green light will appear next to 'Power' display on the device. A red or orange light indicates you need to re-charge. Included in your R52A6A package is an AC-Adapter. Alternatively, you can use a USB cable to charge/re-charge your device (sold separately).

Opening the Browser Interface

How to Connect to the R526A (Windows Users – for MAC Instructions see the next section)

1. Turn on the R526A and ensure your WiFi is enabled on your PC or laptop. You can view your available wireless networks by going through the control panel, network connections or system tray (lower right hand corner of your screen).

2. Select “FRANKLIN_R526A XXXX” as your wireless network.

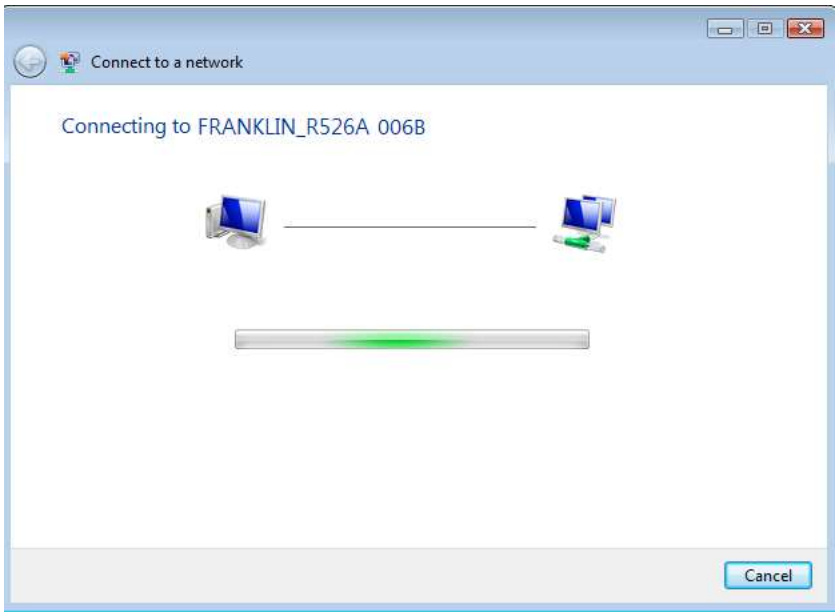
Note.

The last 4 digits, ‘XXXX’ of the SSID is the last four digits of your MAC address. You can find the MAC address of your R526 on the label under the battery.

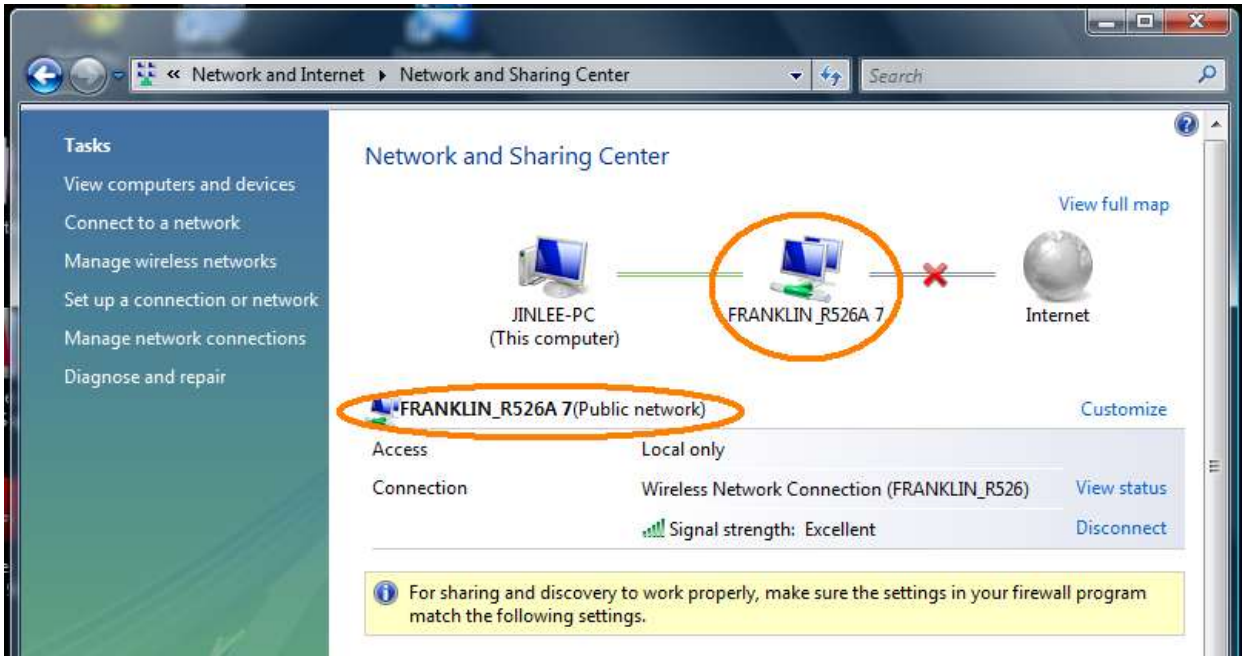
.

3. Click *Connect*.

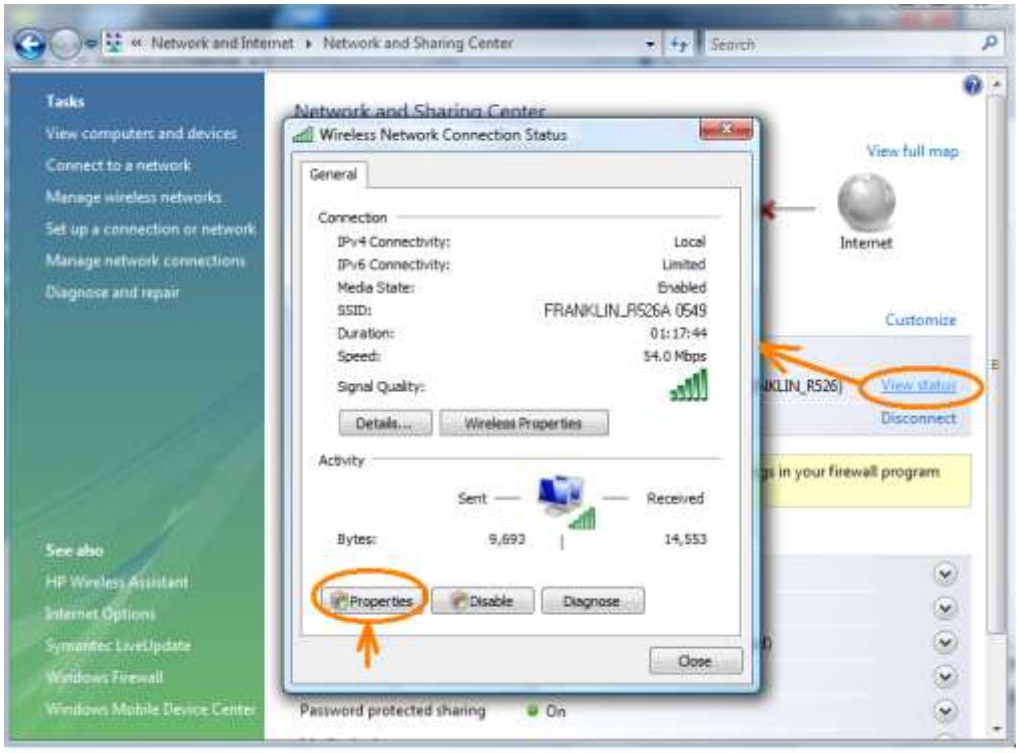
The default security for the R526A is WEP 64-bit. The default security key is “12345.” Enter 12345 to continue connecting to the R526A. If you would like to change this security setting after you have activated your device, see the WiFi > Security setting of this document for changing security settings.

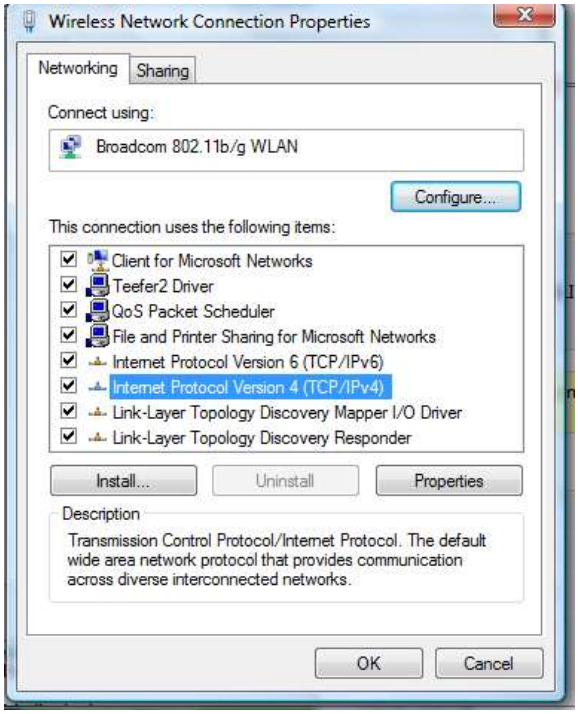


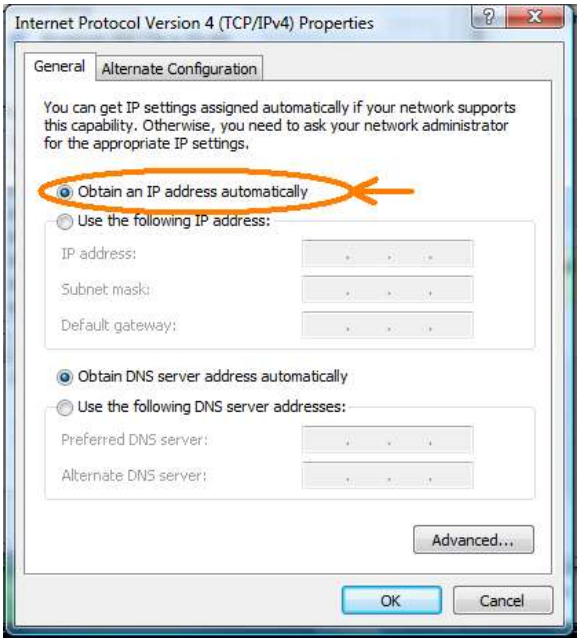
4. When connected to the R526 you will see the connection as 'FRANKLIN_R526A XXXX' – as shown below.



5. Before proceeding, ensure your wireless connection properties are set to 'Obtain an IP Address Automatically.' For Windows XP and Vista 32-bit users, you can right-click on your wireless network, select properties, then TCP/IP properties. For Windows Vista 64-bit and Windows 7 users, you can click on 'View Status' as shown below


Network and Internet ▸ Network and Sharing Center
Search
Tasks
View computers and devices
Connect to a network
Manage wireless networks
Set up a connection or network
Manage network connections
Diagnose and repair
Network and Sharing Center
View full map
Internet
Customize
View status
Disconnect
Wireless Network Connection Status
General
Connection
IPv4 Connectivity: Local
IPv6 Connectivity: Limited
Media State: Enabled
SSID: FRANKLIN_R526A 0549
Duration: 01:17:44
Speed: 54.0 Mbps
Signal Quality:
Details...
Wireless Properties
Activity
Sent
Received
Bytes: 9,693 14,553
Properties
Disable
Diagnose
Close
See also
HP Wireless Assistant
Internet Options
Symantec LiveUpdate
Windows Firewall
Windows Mobile Device Center
Password protected sharing
On


Wireless Network Connection Properties
Networking
Sharing
Connect using:
Broadcom 802.11b/g WLAN
Configure...
This connection uses the following items:
Client for Microsoft Networks
Teefer2 Driver
QoS Packet Scheduler
File and Printer Sharing for Microsoft Networks
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Link-Layer Topology Discovery Mapper I/O Driver
Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
OK
Cancel



6. Next, open your web browser to *http://192.168.5.1*. This will bring you to the web user interface of the R526A.

Device Activation (Windows)

If your device has not been activated at time of purchase, you must activate now.

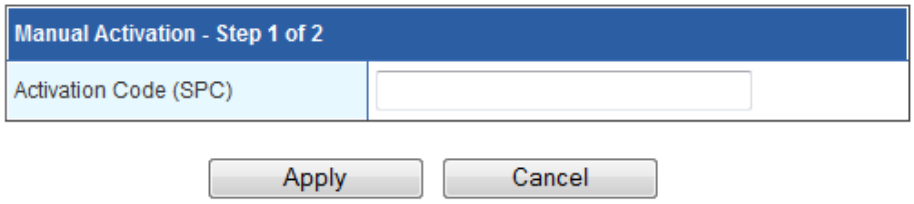
Before you activate, you need SPC, MDN and MIN from the Carrier providing the service.

Click *Login* button. You will be prompted to enter your username and password. The default Username and Password is admin/admin.

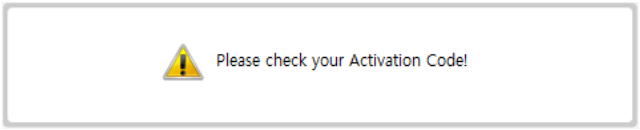
Click *OK*. Then, you will see the pop up screen requiring Manual Activation.

Activation process consists of 2 steps.

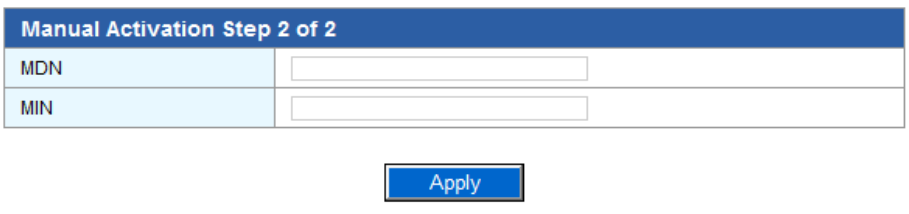
- 1st step is to input SPC. Input six '000000' for SPC (the SPC can be unique to the Carrier, confirm with your own Carrier before attempting to activate) and click *Apply.*



If the Activation Code is incorrect, you will be asked to try again. If the Activation Code is correct, proceed to the 2nd step.



- 2nd step is to input MDN and MIN.



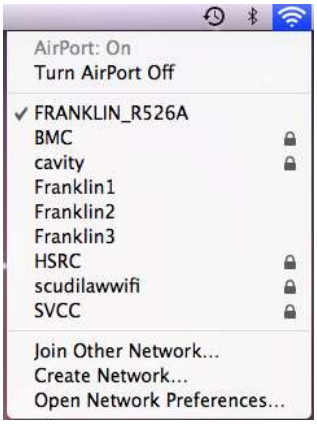
Input the 10 digit MDN (Mobile Directory Number) and MIN (Mobile Identification Number) then click *Apply.* The MDN and MIN are provided by your carrier. Please contact your carrier for the correct MDN and MIN.

Device Activation (Mac Users Only)

1. Go to Airport Icon at the right upper corner of desktop tap menu and click to open.

Airport on  **Airport off** 

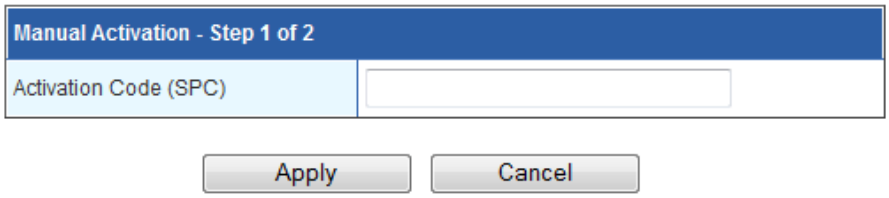
Ensure your Airport mode is turned on to allow your computer to search for available WiFi networks.



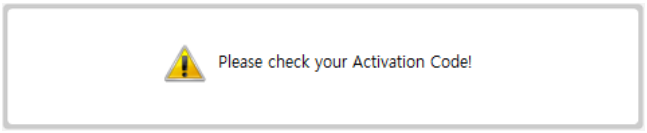
2. Choose “Open Network Preferences” on the drop-down menu and select “FRANKLIN_R526A XXXX” of your Wi-Fi network and apply it.

3. Now that you are connected, the Activation process consists of 2 steps.

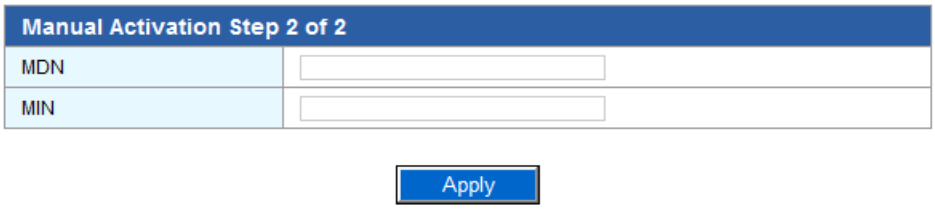
- 1st step is to input SPC. Input six '000000' for SPC (the SPC can be unique to the Carrier, confirm with your own Carrier before attempting to activate) and click *Apply.*



If the Activation Code is incorrect, you will be asked to try again. If the Activation Code is correct, proceed to the 2nd step.



- 2nd step is to input MDN and MIN.



Input the 10 digit MDN (Mobile Directory Number) and MIN (Mobile Identification Number) then click *Apply.* The MDN and MIN are provided by your carrier. Please contact your carrier for the correct MDN and MIN.

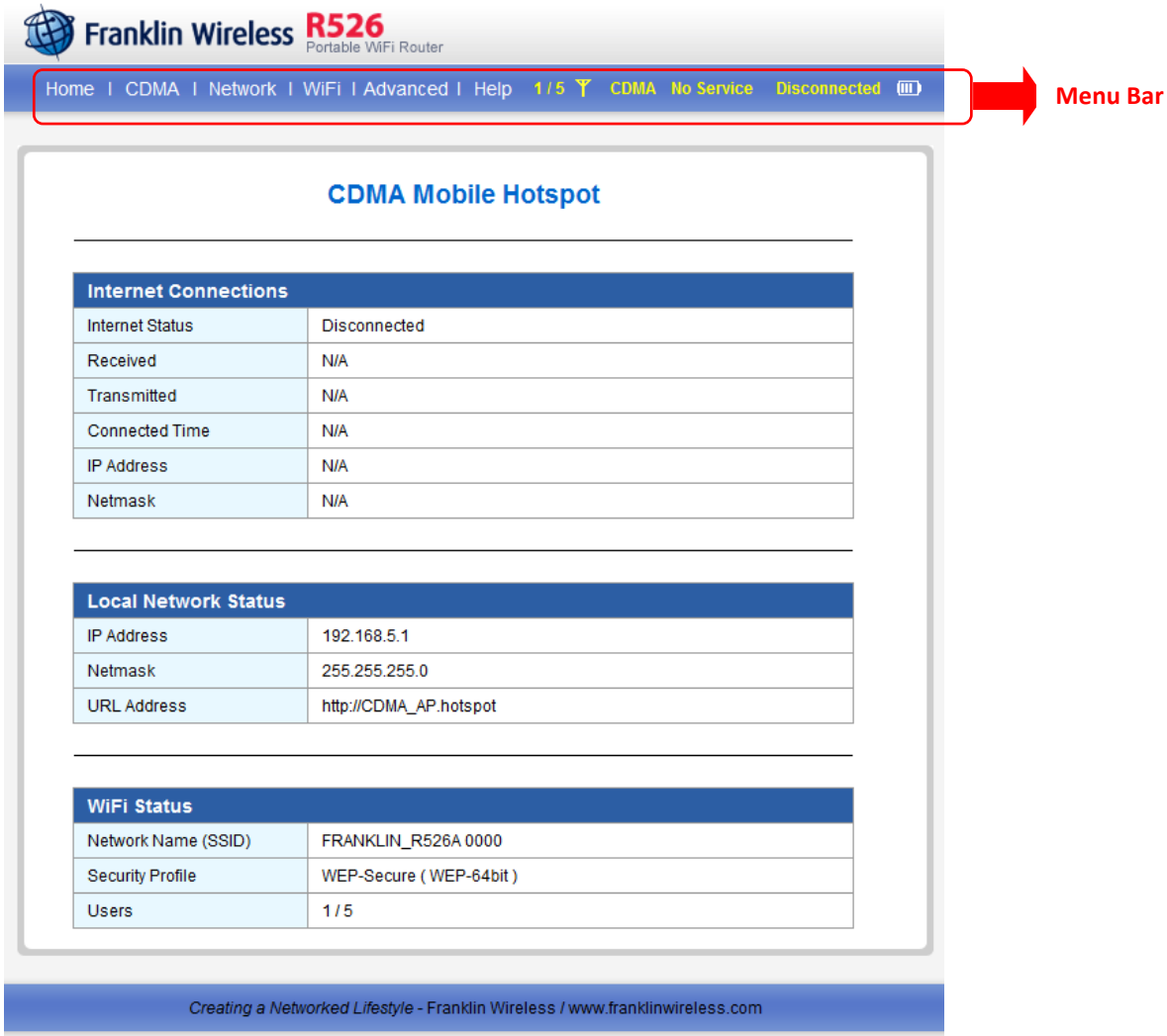
The Browser Interface and Settings

Open your Web browser and enter *http://192.168.5.1/*or *http://cdma_ap.hotspot/* into the address window. The browser interface will open.

Your CDMA and WiFi use a browser interface to configure the device.

The browser interface lets you:

- View the status of aspects of your network.
- Set up DHCP, WEP or WPA security, MAC filtering, port filtering, port forwarding, DMZ, and VPN pass through.
- Set up a hotspot to allow a maximum of five connections to your device without having to share your network name and network key.



Home

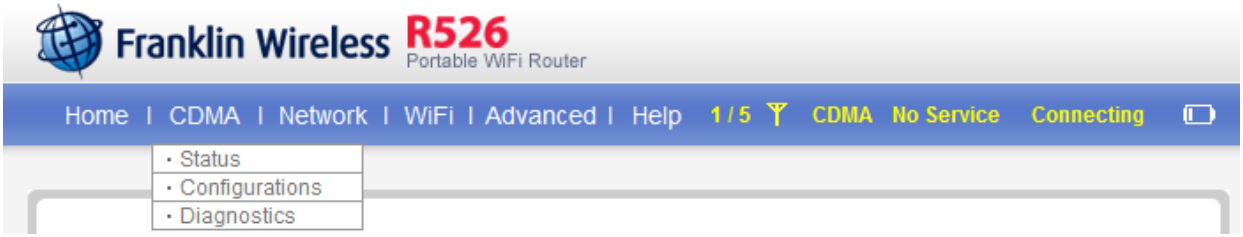
The Home screen is the first screen you see after logging in to the browser interface. It is the main point of entry for all your work in the browser interface. The menu bar runs horizontally along the top of the browser interface.

It shows how many users or WiFi embedded devices are connected. It also displays information about your device's connection strength and battery level.

CDMA

The CDMA menu allows you to set your authentication or CDMA auto connection option.

It also provides internet connection information as well and traffic counters.



- *Status*

The CDMA status screen is divided into two sections.

The Internet Connections section displays the following information:

- Duration of the current connection.
- Roaming status.
- Current data bytes of received or transmitted.
- Connected time.
- The device's IP address and subnet mask.
- Gateways IP address.
- DNS server's IP address.

Internet Connections	
Internet Status	Disconnected Connect
Connection Status	Disconnected
Roaming	Home
Received	N/A
Transmitted	N/A
Connected Time	N/A
IP Address	N/A
Netmask	N/A
Gateway	N/A
DNS	N/A

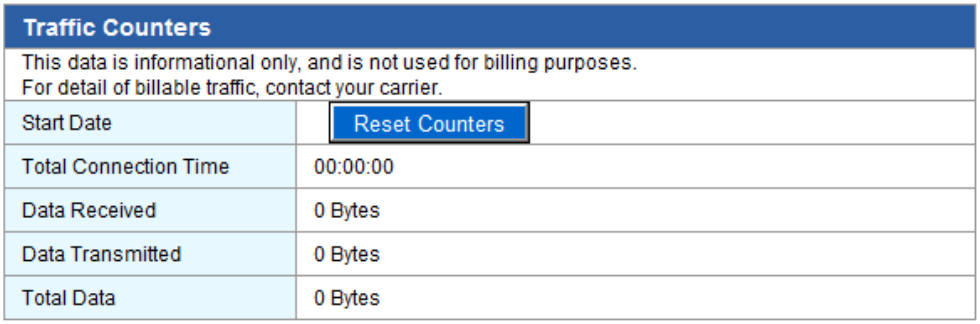
Click *Connect* to connect to your 3G network.

It will not normally require any additional configuration to the basic settings unless you are using the device behind a corporate firewall, and this may require the appropriate proxy server settings to be modified.

The Traffic Counters section also displays the following:

- Date and time connection was made.

- Total duration of connection.
- Total data bytes received and transmitted.
- Total data bytes for both directions.

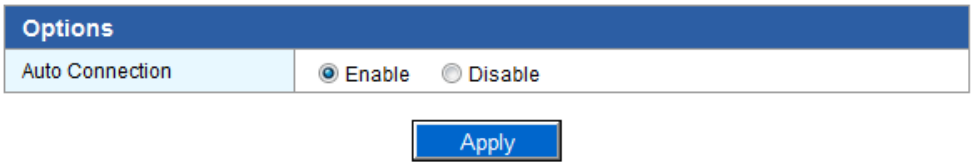


This section displays a count for the device's usage information.

Click *Reset Counters* to initialization of counters.

- *Configurations*

The Configurations menu allows you to set *auto connection.* This function allows your device to connect to your 3G network automatically when it is turned on.

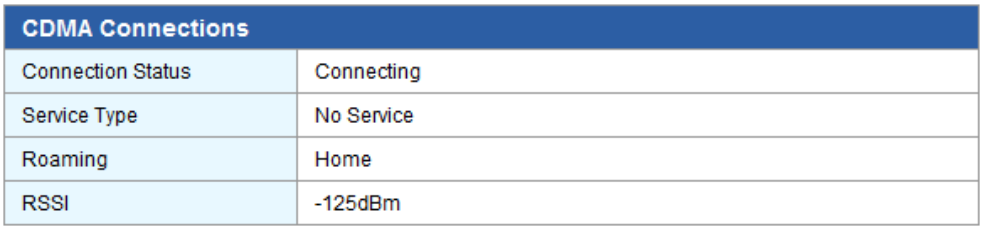


- *Diagnostics*

The Diagnostics menu gives you the 3G modem information, and this screen is divided into two sections.

The CDMA Connections section displays the following:

- CDMA status information.
  (ex. Network Searching, Connecting, Connected, Disconnecting, Disconnected, or Dormant)
- Service type. (ex. 1xRTT, EVDO Rev.A, EVDO Rev.0, or No Service)
  - EVolution-Data Only or EVolution-Data Optimized(EVDO): Telecommunications standard for the wireless transmission of data through radio signals.
- Current roaming status.
- Received Signal Strength Indication(RSSI) – RSSI is device's connection strength.

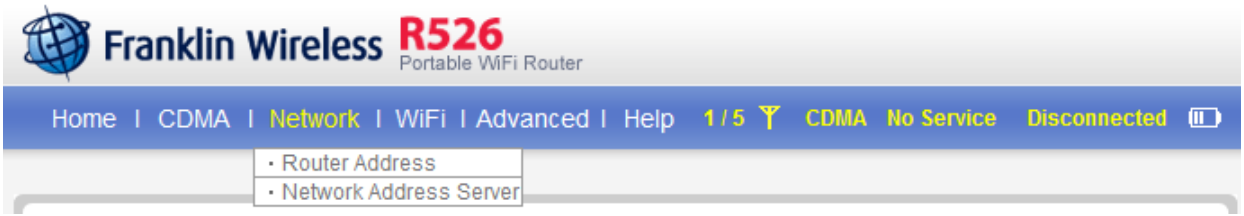


The CDMA Modem section displays the following:

- Device's manufacturer.
- Device's model name.
- Device's CDMA firmware version in use.
- Electronic Serial Number(ESN).
- Mobile Equipment IDentifier(MEID).
- Mobile Directory Number(MDN).
- PRL version in use.

CDMA Modem	
Manufacturer	FRANKLIN
Model	R526a
Firmware Version	R526AC_
ESN	00000000
MEID	00000000000000
MDN	
PRL Version	10003

Network



The Network menu allows you to set domain name of the wireless browser interface and set DHCP.

- *Router Address*

This Router Address menu gives you following status information:

- IP address and subnet mask of the wireless browser interface.
- Device's MAC address.
- The wireless browser interface's current URL address. (which can be change.)

Local Network Setup	
IP Address	192.168.5.1
Netmask	255.255.255.0
MAC Address	00:07:79:07:00:00
URL Address	http://CDMA_AP .hotspot

Apply

- *Network Address Server*

This menu allows you to modify WiFi DHCP IP range.

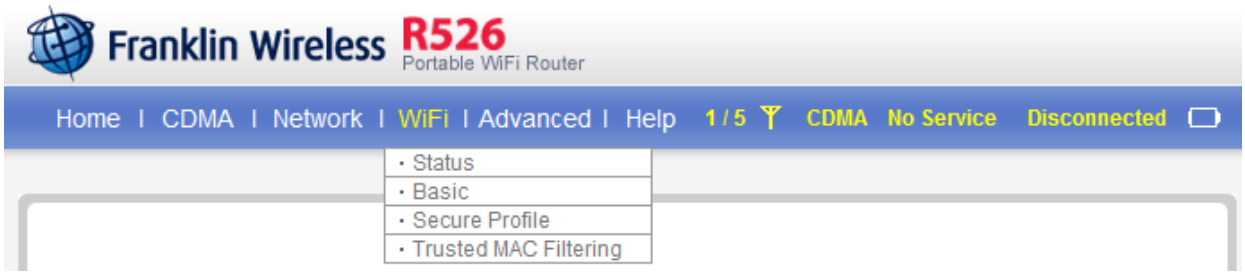
Local Network Setup	
DHCP Server	Enable
DHCP IP Range	192. 168. 5. 100 ~ 110

Apply

- DHCP Server: Enabling the DHCP server allows the device to automatically assign a local IP address to a new device joining your network (such as a wireless printer or an additional laptop). When the DHCP server is disabled, you will have to assign static IP addresses to all devices on your network.

WiFi

The WiFi menu allows you to view status information for your WiFi network and configure your hotspot.



- *Status*

This Status menu gives you following status information:

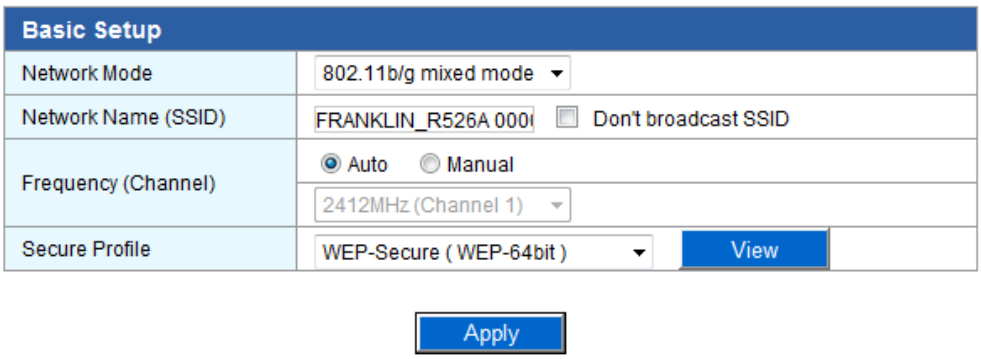
- Network Name. (also known as SSID)
- Security profile in use.
- Users(clients) information currently connected to the device.

WiFi Status	
Netwok Name (SSID)	FRANKLIN_R526A 0000
Security Profile	WEP-Secure (WEP-64bit)

WiFi Clients		
Host name	MAC Address	IP Address
JeonjaeYoung-PC	5C:AC:4C:07:0D:64	192.168.5.101

- *Basic*

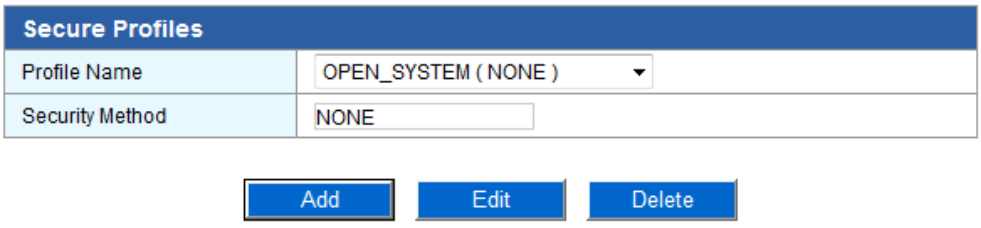
This menu allows you to modify WiFi and Secure Profile.



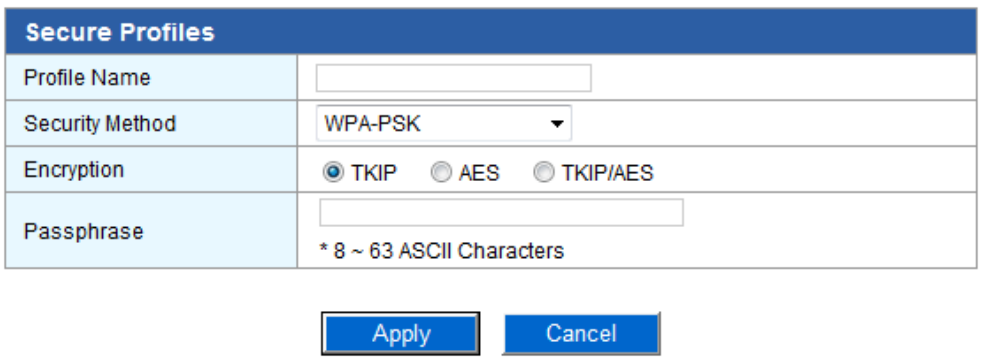
- Network Mode: The type of wireless networking you are currently using. You can choose either mode among 802.11b only, 802.11g only, 802.11b/g mixed mode. The default mode is 802.11b/g mixed mode.
- Network Name (SSID): You can change or input new Network Name (SSID). System default SSID is FRANKLIN_R526A XXXX - XXXX is your device's MAC address number last four characters. If you check *Don't broadcast* box, WiFi clients who try to access the CDMA mobile hotspot can not see this SSID.
- Frequency (Channel): The radio channel is divided into Auto and Manual. This should be usually set to Auto and left unchanged. Available channels are Auto and 1 to 11.
- Secure Profile: The type of security the router is using. This applies to the Secure and the Temporary hotspot profiles. You can modify(add/edit/delete) Secure Profile using *View* button.

- *Secure Profile*

This menu allows you to modify(add/edit/delete) Secure Profile.



Click *Add*, define Secure Profile. You can set Profile Name, Security Method, Encryption, and Passphrase.



- WPA-PSK/WPA2-PSK: New WiFi certification program mode.

- WEP(64bit or 128bit): Traditional WiFi certification program mode.
- TKIP/AES: Data encryption mode.

1. Select a Security Method from the security list.
2. Select the Encryption mode.
3. Enter a new network key in the Passphrase box. (Permissible characters are listed in gray just under the box.)
4. Click *Apply*.

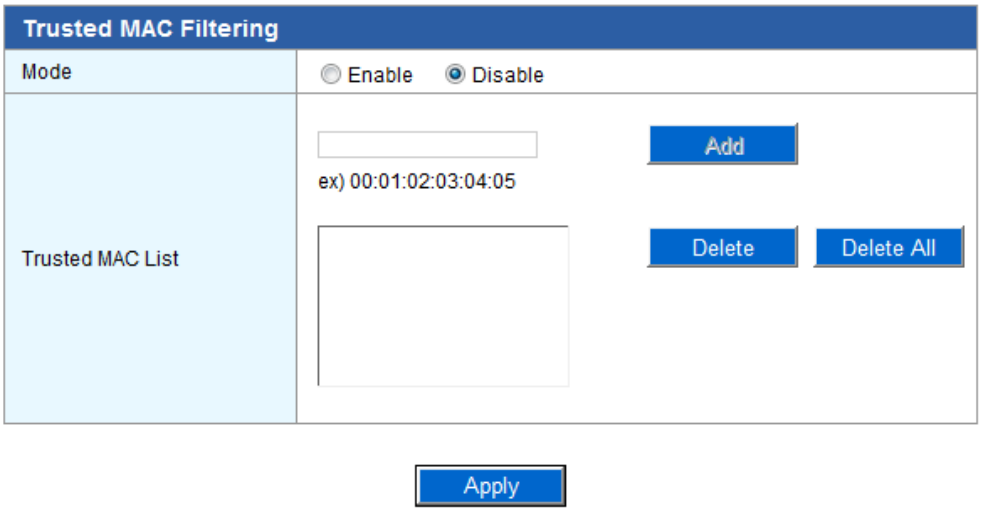
Click *Edit,* you can redefine Security Profile. Also click *Delete*, delete Security Profile from the security list. But you can not *Edit* or *Delete* to *OPEN_SYSTEM (NONE)* Profile. This profile has set as the default Secure Profile.

Note.

When you click Apply, you will need to reconnect to your router by closing your current view and re-opening a browser connection to http://192.168.5.1/

- *Trusted MAC Filtering*

MAC Filter allows you to limit access to your device to only those devices with a specified MAC address (a unique code assigned to hardware such as network adapters).



Finding the MAC Address

The MAC Address is also known as a hardware or physical address for a device, usually a network adapter.

It consists of six pairs of numbers and letters (for example, 00:21:9B:1C:64:34).

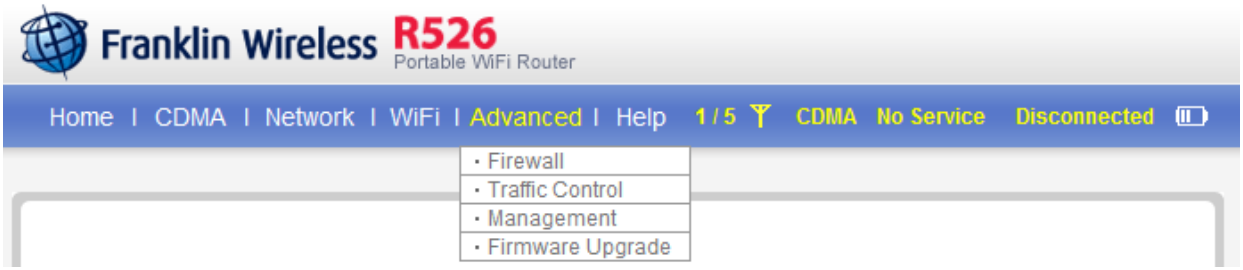
You can view the MAC address for any device connected to the CDMA Mobile device in the WiFi Clients section of the WiFi Status screen. (See “WiFi Clients” on page 14.)

Note.

When you enable this feature for the first time, ensure you add your wireless MAC first, then click Apply.

Advanced

This menu allows you to configure your device to enable Port Filtering, VPN Passthrough, Port Forwarding, DMZ, Backup Configuration, Power Saving, Firmware Upgrade, and so on.

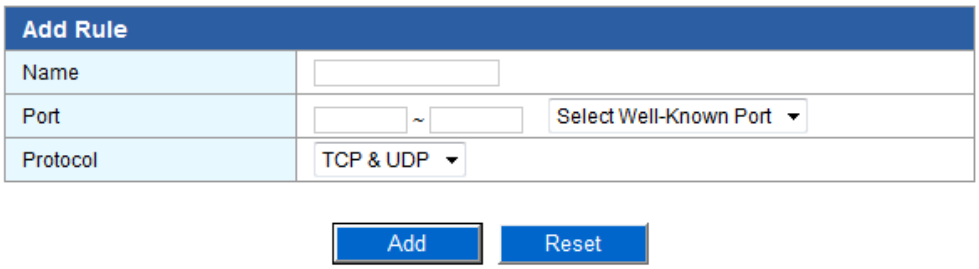


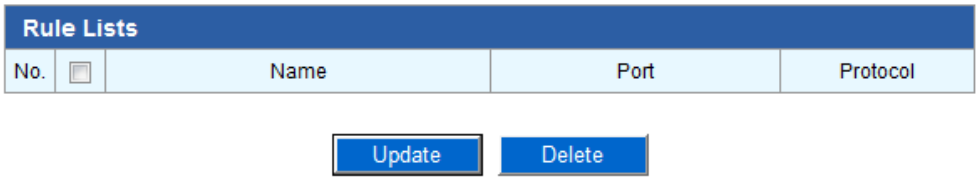
- *Firewall*

The *Firewall* menu allows you to set Port Filtering and VPN Passthrough function.

1) Port Filtering

Port filtering allows you to conserve bandwidth by preventing non-business applications from accessing the Internet, and to prevent applications such as online games from accessing the Internet.





1. Selecting the list box for the applications for which you want to allow access to the Internet.
2. or enter the application value in the Name, Port, and Protocol boxes.
3. Click *Apply*.

2) VPN Passthrough

VPN Passthrough is required if you are going to connect to a VPN.

(Such as a corporate system.)

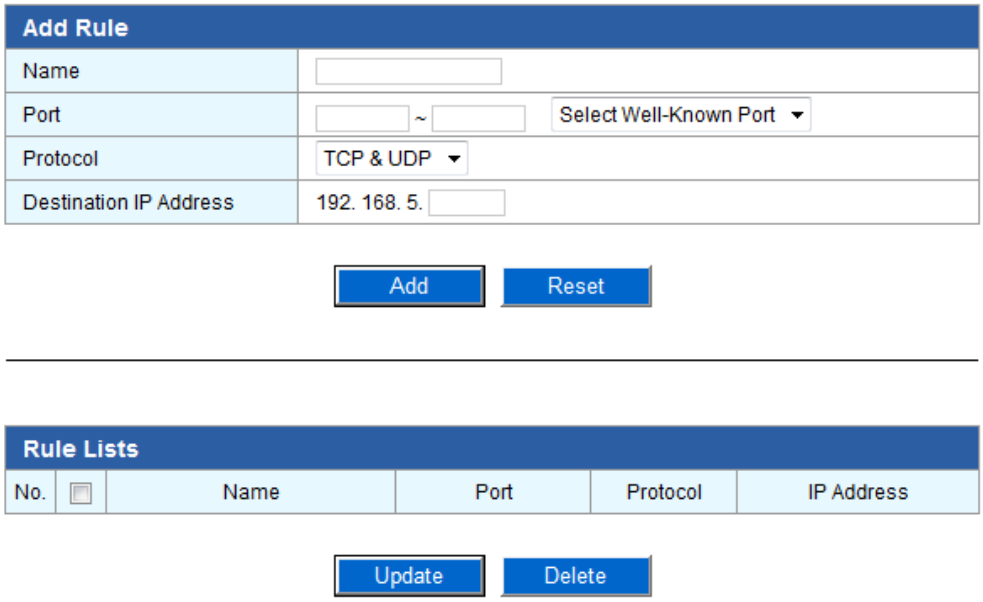
- L2TP/IPSEC/PPTP: VPN tunneling protocols.

- *Traffic Control*

This menu allows you to set Port Forwarding and DMZ function.

1) Port Forwarding

Port forwarding allows designated users or applications to reach specified servers, such as FTP and DNS servers, on your computer. Also, some online games require incoming access to work properly.



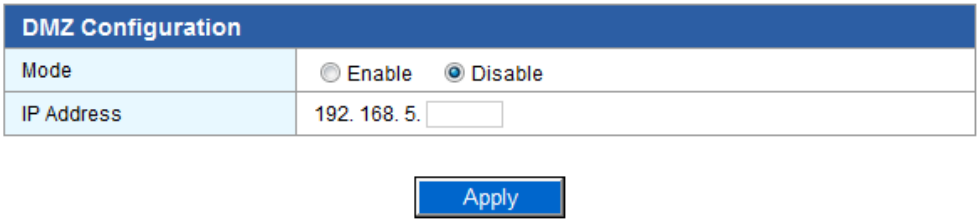
1. Selecting the list box and typing local static IP address of the device hosting the application IP.
2. or enter the value in the Name, Port, Protocol, and Destination IP Address boxes.
3. Click *Apply*.

Note.

You cannot use port forwarding with some standard data accounts. To use port forwarding, you may need to request a static IP address from your carrier / service provider..

2) DMZ

DMZ function is a host on the internal network that has all ports exposed, except those ports otherwise forwarded. The Mode set enable and enter the local static IP address.



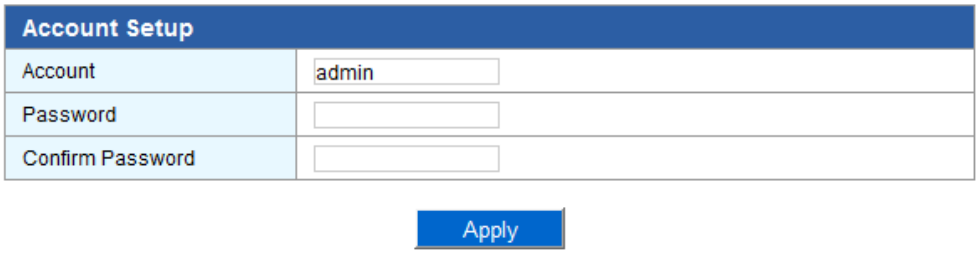
- *Management*

You can create a new administrator's name and password. Also you configure your device to apply Backup Configuration, Power Saving, and Firmware upgrade in this category.

Note.

When you change the default settings, keep you new information in a safe place.

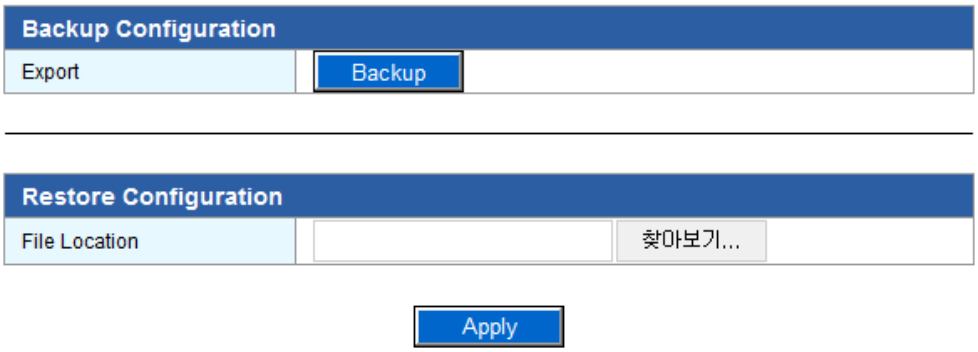
1) Account



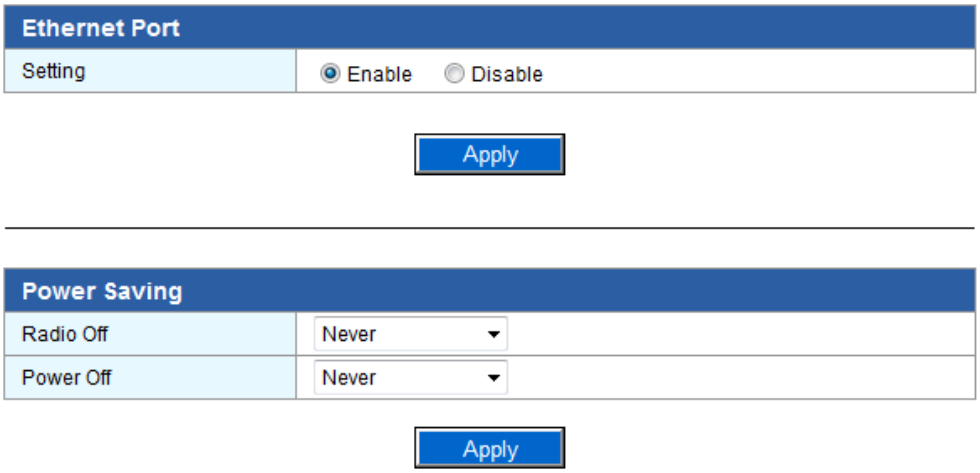
Create administrator's name and password.

2) **Backup & Restore**

The Backup Configuration allows you to backup your settings save to your PC, memory stick, CD, etc. And the Restore Configuration allows you to restore previously saved/backed up settings.



3) Power Management



- Ethernet Port: You can set mode of the Ethernet port. Enable mode allows you to connect of using Ethernet cable (UTP cable).
- Radio Off: You can use the Radio Off mode to customize your device to switch to a low power mode when not in use. There are 10 minute increments from 10-60 minutes. Select *Never* to disable this power saving feature. If you want to switch the WiFi Radio on earlier than the time you set in this menu, you can easily push the power button one time lightly. A blue WiFi LED of indicates that CDMA Mobile device is ready to connect.
- Power Off - The Power Off mode allows you to choose when your device will automatically power off, to save battery life, due to inactivity. There are 10 minute increments from 10-60 minutes you can select. Select *Never* to disable this power saving feature.

4) Factory Default

Click *Update* to reset your device to the defualt factory settings.

- *Firmware Upgrade*

You can upgrade your device's configuration file to your computer. (The Version is showed current WiFi firmware version.)

Help

Help menu gives you the information about customer service, the Quick Start Guide, full User Guide, Frequently Asked Questions, & Troubleshooting.

- *User Guide*
- *QSG*

Part 2

Warranty

Manufacturer's Limited One-Year Warranty:

Franklin Wireless (the company) warrants to the original retail purchaser of this device, that should the product or any part thereof, during normal consumer usage conditions, be defective in material or workmanship that results in product failure within the first twelve (12) month period from the date of purchase, such defects will be repaired or replaced, with a new or refurbished product at the Company's discretion, without charge for parts and labor directly related to the defect(s). This warranty extends to consumers who purchase the product in the United States, Mexico, or Canada and it's not transferable or assignable. This warranty does not apply to:

(a) Product subject to abnormal use or conditions, accident, mishandling, neglect, unauthorized alteration, misuse, improper installation or repair or improper storage;

(b) Products whose mechanical serial number or electronic serial number has been removed, altered, or defaced;

(c) Damage from exposure to moisture, humidity, excessive temperature or extreme environment conditions;

(d) Damage resulting from connection to, or use of any accessory or other product not approved or authorized by the company;

(e) Defects in appearance, cosmetic, decorative or structural items such as framing and non-operative parts;

(f) Product damaged from external causes such as fire, flooding, dirt, sand, weather conditions, battery leakage, blown fuse, theft or improper usage of any electrical source.

The Company disclaims liability for removal or reinstallation of the product, for geographic coverage, for inadequate signal reception by the antenna or for communications range or operation of the cellular system as a whole.

When sending your wireless device to Franklin Wireless' authorized distributions for repair or service, please note that any personal data or software stored on the device may be inadvertently erased or altered. Therefore, we strongly recommend you make a back up copy of all data and software contained on your device before submitting it for repair or service. This includes all contact lists, downloads (i.e. third-party software applications, games and graphics) and any other data added to your device. Franklin Wireless is not

responsible for and does not guarantee restoration of any third-party software, personal information or memory data contained in, stored on, or integrated with any wireless device, whether under warranty or not, returned to Franklin Wireless' authorized distributors for repair or service. To obtain repairs or replacement within the terms of this Warranty, the product should be delivered with proof of Warranty coverage (e.g. dated bill of sale), the consumer's return address, daytime phone number and/or fax number and complete description of the problem, transportation prepaid, to the Company at the address shown below or to the place of purchase for repair or replacement processing. In addition, for reference to an authorized Warranty station in your area, please call (800)959-3558 in the United States.

The extent of the company's liability under this warranty is limited to the repair or replacement provided above and, in no event, shall the company's liability exceed the purchase price paid by purchaser for the product.

Any implied warranties, including any implied warranty of merchant ability or fitness for a particular purpose, shall be limited to the duration of this written warranty. Any action for breach of any warranty must be brought within a period of 18 months from date of original purchase, but in no case shall the company be liable for a special consequential or incidental damages for breach of this or any other warranty, express or implied, whatsoever. The company shall not be liable for the delay in pending service under this warranty or loss of use during the time the produce is being repaired or replaced.

No person or representative is authorized to assume for the Company any liability other than expressed herein in connection with the sale of this product.

Some states or provinces do not allow limitations on how long an implied warranty lasts on the exclusion or limitation of incidental or consequential damage so the above limitation or exclusions may not apply to you. This Warranty gives you specific legal rights, and you may also have other rights, which vary from state to state or province to province.

Franklin's Authorized Service Center Address:
6205 Lusk Blvd
San Diego, CA 92121

Q: What is the R526A's main purpose unlike other routers?

A: The R526A is a portable WiFi router that fits in the palm of your hand. It will allow you to connect up to 5 devices to access the internet, such as laptops, digital cameras, portable game consoles or mobile phones.

Q: What networks does the R526A operate on?

A: The R526A operates on 3G wireless networks.

Q: What are the air holes on the both side of the R526A?

A: The air holes are designed to reduce the heat generated by the device itself while it used. Keep the device away from open flames, dusty conditions, and keep it dry for optimal performance.

Q: What kind of security is available with the R526A?

A: The R526A supports advanced WiFi security protocol through standard methods such as WiFi Protected Access (WPA & WPA2) and the previous method of Wired Equivalent Privacy (WEP).
More advanced settings are available in the Web based user interface.

Q: What if the user forgets their R526A password?

A: The R526A can be reset by powering on the device, remove the battery cover, and depress the small button near the bottom of the battery using a paper clip or pen and hold for 3 seconds. The Power LED will turn off-and-on twice to indicate reset is successful. The unit will power up with the factory default configuration.

Q: What might the owner of the R526A need to be aware of before sharing with multiple devices?

A: With multiple devices or used as a temporary hotspot:

- If there are several heavy data users on at the same time, you may notice a degradation in performance
- Users are not allowed to access more than 5 devices to the R526A in order to keep the devices' data speed stable enough to be communicated without a problem.
- Be aware these users are contributing to your data usage. You may want to check your account online to see how much of a difference it is making and how close you are to any usage caps that may apply under your Franklin wireless network connection plan.
- If all are accessing a R526A that is using the battery, the battery will drain faster than the average of 3 hours usage time for one user.

Q: Can a user connect the R526A to their computer with a USB cable?

A: When the R526A is tethered via a USB cable to a computer, the device will not function as a hotspot. In this mode the R526A can be charged, or re-charged only.

Q. What is the LAN port of R526A can be used for?

A: The LAN Port of the R526A is users who have a laptop or desktop computer which does not have WiFi capability.

Q: What is the average battery usage time?

A: The battery will have on average 3 hours of active use time when connected to a single device and will discharge more rapidly as additional devices are connected (up to 5 WiFi devices are acceptable). There is 7.5 hours of standby time.

Q: Why the R526A turns off while in used and it wouldn't turn on again?

A: The red solid power LED indicates the battery is below 20% and if it's blinking, it indicates the R526A will turn off very soon. After the battery has run down, it turns off automatically. So you need to charge the battery using AC-DC adaptor.

Please refer to the Quick Start Guide on page 9.

Q: How close does the user's WiFi enabled device need to be from the R526A?

A: The device will need to be within 16 feet or 5 meters of the WiFi device to work. So a user can keep the R526A in their pocket, laptop bag, or sitting on a desk or window ledge across a room (for better coverage).

Q: Does the R526A support voice calls, fax and/or text messaging?

A: Voice calls, text messaging and fax are not supported.

Q: Can the R526A be used for memory storage?

A: The R526A does not support onboard or removable memory storage.

Q: How long does a user need to charge the battery before they begin using?

A: The battery must be fully charged before using the R526A for the first time. We recommend a minimum of 2 hours charging time before first use. After the initial use and set-up, you may use with the battery alone or with the battery and the AC power. The R526A can also be charged/re-charged by connecting the device to your computer via a USB cable (sold separately).

Q: Does the R526A require software installation?

A: The R526A comes with a browser URL that allows the user to configure the device.

You can activate, select a profile, establish security and set more advanced settings without installing any software.

Q: What does the user of the R526A need to begin to do configuration and activation?

A: See section 1 of this manual for activation instructions.

Q: What if the R526A can not access the internet even though the unit has been activated?

A: Verify your network & signal strength for optimal performance.

Q: When will a user of the R526A need to access the browser interface?

A: The R526A browser interface will only need to be accessed or used when configuring your device for the first time or changing the security settings or establishing more advanced settings.

Q: Why does the R526A gets warm?

A: The R526A has two radios inside: the 3G CDMA radio and the WiFi radio. In fringe areas of low 3G coverage, the transmit power will be at the max and therefore generate more heat. The device has been environmentally tested and approved by the FCC.

Part 4

Glossary

Franklin Wireless

- **802.11 (b, g, n)** — A set of WLAN communication standards in the 2.4, 3.6 and 5 GHz frequency bands.
- **Access Point (AP)** — A device that allows wireless communication devices to connect to a wireless network using a standard such as WLAN.
- **DHCP** — Dynamic Host Configuration Protocol. A network application protocol used to obtain configuration information for an Internet Protocol network.
- **DHCP Server** — A server that uses DHCP to obtain configuration information for operation in an Internet Protocol network.
- **DNS** — Domain Name System. A system for converting host names and domain names into IP addresses on the Internet or on local networks that use the TCP/IP protocol.
- **ESN** — Electronic Serial Number. A unique 32-bit number embedded in a wireless device that identifies the device.
- **MEID** — Mobile Equipment Identifier. The unique second-generation serial number assigned to the R526A for cellular network use.
- **Firmware** — A program that internally controls an electronic device.
- **FTP** — File Transfer Protocol. A network protocol for exchanging files over a TCP network.
- **Gateway** — A network point that acts as an entrance to another network that uses a different protocol.
- **Host Name** — The unique name by which a network-attached device is known on a network.

● **Hotspot** — A WLAN access point or area for connecting to the Internet.

● **HTTP** — Hypertext Transfer Protocol. An application-level protocol for accessing the World Wide Web over the Internet.

● **IP address** — Internet Protocol address. The address of a device attached to an IP network (TCP/IP network).

● **LAN** — Local Area Network. A type of network that lets a group of computers, all in close proximity (such as inside an office building), communicate with one another.

● **MAC Address** — A number that uniquely identifies a given network adapter on a LAN. MAC addresses are 12-digit hexadecimal numbers.

● **MIN** — Mobile Identification Number. It refers to the 10-digit unique number that a wireless operator uses to identify the mobile phone. A MIN is a number that uniquely identifies a mobile working under TIA standards for Cellular and PCS technologies

● **MSID** — Mobile Station ID. A number provisioned by a service provider to a mobile phone that identifies that phone to the network.

● **MSL** — Master Subsidy Lock. A numeric code for accessing certain phone settings.

● **NAI** — Network Access Identifier. A standard way of identifying users who request access to a network.

● **Network Mask** — A number that allows IP networks to be subdivided for security and performance.

● **NNTP** — Network News Transfer Protocol. An Internet application protocol for reading and posting Usenet (newsgroup) articles.

● **POP** — Post Office Protocol. An Internet protocol for retrieving email from a remote server over a TCP/IP connection.

● **Port** — A virtual data connection used by programs to exchange data.

● **Port Forwarding** — A process that allows remote devices to connect to a specific computer within a private LAN.

● **Port Number** — A number assigned to a user session and server application in an IP network.

● **Protocol** — A standard that enables connection, communication, and data transfer between computing endpoints.

● **PPTP** — Point-to-point Tunneling Protocol. A method for implementing virtual private networks that does not provide confidentiality or encryption.

● **PRL** — Preferred Roaming List. A list that your wireless phone or device uses to determine which networks to connect with when you are roaming.

● **RFB** — Remote Frame Buffer. A protocol for remote access to graphical user interfaces.

● **Router** — A device that connects two networks.

● **RTP** — Real-time Transport Protocol. A packet format for streaming multimedia over the Internet.

● **SMTP** — Simple Mail Transfer Protocol. An Internet standard for email transmission across IP networks.

● **SSID** — Service Set Identifier. The name assigned to a WLAN network.

● **TCP** — Transmission Control Protocol. A core protocol for transmitting and receiving information over the Internet.

● **TCP/IP** — Transmission Control Protocol/Internet Protocol. A communications protocol developed under contract from the U.S. Department of Defense to internetwork dissimilar systems.

● **Telnet** — Telecommunication Network. A network protocol used on the Internet or on local area networks.

● **TFTP** — Trivial File Transfer Protocol. A file transfer protocol with a subset of FTP functionality.

● **UDP** — User Datagram Protocol. A simple transport protocol used to transfer information on the Internet.

● **VNC** — Virtual Network Computing. A graphical desktop sharing system that uses the RFB protocol to remotely control another computer.

● **VPN** — Virtual Private Network. A secure private network that runs over the public Internet.

● **VPN Passthrough** — A feature that allows a client to establish a tunnel only with a specific VPN server.

● **WAN** — Wide Area Network. A public network that extends beyond architectural, geographical, or political boundaries (unlike a LAN, which is usually a private network located within a room, building, or other limited area).

● **WEP** — Wired Equivalent Privacy. An IEEE standard security protocol for 802.11 networks. Superseded by WPA and WPA2.

● **WLAN** — Wireless Fidelity. Any system that uses the 802.11 standard developed and released in 1997 by the IEEE (Institute of Electrical and Electronics Engineers).

● **WLAN Client** — A wireless device that connects to the Internet via WLAN.

● **WLAN** — WLAN LAN. A typically low-power network that transmits a wireless signal over a span of a few hundred feet and usually only to stationary devices.

● **WPA/WPA2** — WLAN Protected Access. A security protocol for wireless 802.11 networks from the WLAN Alliance.

● **WWAN** — Wireless Wide Area Network. Wireless connectivity to the Internet achieved using cellular tower technology. This service is provided through cellular providers. WWAN connectivity allows a user with a laptop and a WWAN device to surf the Internet, check email, or connect to a virtual private network (VPN) from anywhere within the regional boundaries of the cellular service.